

DIGITAL ENCRYPTION STANDARD USERS GROUP

Phone (716) 753-2654

August 8, 1986

NEWSLETTER # 9

DRAWER 1065

CHAUTAUQUA, NY 14722

A MIDSUMMER NIGHT'S DREAM:

Well now, not really a dream though it is midsummer, but rather a "how goes it report" from the fortune cookie factory. The Chautauqua Yacht Club is keeping the Commodore busier than a one-armed sail trimmer. Labor Day will be the end of our yacht club's 1986 sailboat racing season, so we can return to full time DESUG activities in a few weeks (at offices abroad).

TMS7000 SERIES EDITOR/ASSEMBLER:

Considerable progress is being made towards disassembling the source code in U7's 4K ROM. You will recall that U7, a TMS 70C40 microprocessor, has the primary job of decoding the much modified DES encrypted digital audio. By the time you receive this newsletter, Ward Williams will have received a new, highly professional TMS7000 series editor/assembler whose purchase price was donated by three generous DESUG members. It will be of considerable value to Ward's project group.

NEW DESUG OFFICERS:

Dr. Stevens has moved from the position of Chairman of the DESUG Advisory Board to the highly esteemed position of DESUG President and Chief Operating Officer. Bob Cooper is now Chairman of the Advisory Board. Nick Henrison is now VP Engrg. Development and Ward Williams - VP Systems Research. All deserve special thanks from DESUG members for their continuing very significant contributions towards DESUG's goal.

NEW DESUG NEWSLETTER POLICY:

This will be the last newsletter mailed to all of DESUG's membership. Though DESUG does not condone nor encourage nor assist in the violation of any statute of any present or forthcoming descrambling law of the U.S., there are interested firms out there in the vast wasteland with in-house attorneys who would like nothing better than to bring suit against us even though without merit. To make sure this unpleasant happening does not come to pass, the DESUG principals have unanimously voted to discontinue the newsletter for the time being. It is fun, but pointless to tempt our adversaries.

All DESUG communications henceforth will be strictly between the DESUG project leaders and project group members and/or DESUG officers and group members. All DESUG records, lists, and printed matter are now being shredded and turned into kitty litter. Thank you all for your support. We will continue to accept phone calls during business hours. Any future newsletters will be from the DESUG headquarters overseas.

Bob Richardson

11

DIGITAL EMULATION OF STANDARD USER GROUP

Page 11 of 12

REMARKS: A
THAN FOR THE

The following information was obtained from the user group during the digital emulation process. The user group was asked to provide information on their current system configuration, including the operating system, hardware, and software. The information was then used to create a digital emulation of the user group's system. The emulation was then used to test the system and to identify any problems or areas for improvement.

The user group was also asked to provide information on their current system configuration, including the operating system, hardware, and software. The information was then used to create a digital emulation of the user group's system. The emulation was then used to test the system and to identify any problems or areas for improvement.

The user group was also asked to provide information on their current system configuration, including the operating system, hardware, and software. The information was then used to create a digital emulation of the user group's system. The emulation was then used to test the system and to identify any problems or areas for improvement.

The user group was also asked to provide information on their current system configuration, including the operating system, hardware, and software. The information was then used to create a digital emulation of the user group's system. The emulation was then used to test the system and to identify any problems or areas for improvement.

The user group was also asked to provide information on their current system configuration, including the operating system, hardware, and software. The information was then used to create a digital emulation of the user group's system. The emulation was then used to test the system and to identify any problems or areas for improvement.

DIGITAL ENCRYPTION STANDARD USERS GROUP

Phone (716) 753-2654

June 10, 1986

NEWSLETTER # 7

DRAWER 1065

CHAUTAUQUA, NY 14722

Hello DESUG members:

Unfortunate misquoted news releases in IEEE publications and BYTE magazine have driven us up the wall. The phone rings from 6:00 AM till midnight, plus 10 -15 letters per day, with TVRO buffs wanting to join DESUG. Most all are turned down with the polite refrain, "we are accepting applications for membership from professional cryptanalysts."

DESUG welcomes Mr. John Davidson and Mr. Stephen Homer to the fold. DESUG also welcomes Dr. Mark Medress who has requested that his name be added to our newsletter distribution list.

A brief comment about DESUG communications. There are 3 levels of classification; i.e., 1 = none, such as this newsletter: 2= intra-working group letters = restricted: 3 = leader to group member newsletters = private, though other members may receive info copies. DESUG members are asked to respect levels 2 & 3.

Three working groups are concentrating on decapping and micro-probing U7, the TMS70C40 microprocessor with scanning electron microscopes. A caution: the Mode Control (normally pin 36), is internally connected to pin 40, ground. When decapping U7 BE VERY CAREFUL as internal interconnections are easily broken. Suggest that initially U7 only be decapped in the vicinity of pads 36 and 40 and mode control connected only to pin 36. Big thank you to National Semiconductor for this suggestion. When we have U7's ROM disassembled, the source code and pointers in its 128 byte RAM will be distributed to all working groups.

The working groups led by Marc Fine, Bill Ward, and Henry Nicholson are also making great progress. Patent 127 381, Key Distribution System, has been distributed. Call Marc if you need a copy. IBM's Dr. Anon E. Mousse will be assisting Bill Ward's group with the 9 track, 800 BPI, IBM format, data read-out program. Bill has completed Phase 1 (data capture), is now in Phase 2 (capture command & control from U24), and hopes to be into Phase 3 (encrypted audio bit stream separated from command & control), shortly.

Tapping out the VC2000E is not DESUG's fundamental objective. Understanding the complete operating system is DESUG's end objective. This data will NOT be released to the public until a majority of DESUG principals decides it is appropriate.

Bob and Patti Cooper are due back from their honeymoon in the Far East this week. All DESUG members welcome them home.

Bob Richardson

Bob Richardson, DESUG Secretary

Bob's
CALL ME 347-2654
73. Bob

